REMARKS

In response to the Official Action of December 5, 2007, minor correction has been made to correct grammatical errors at page 16 of the specification and minor amendment has been made to claim 1 so as to make clear proper antecedent basis for the chip referred in the receiving action of said claim. Claims 1, 9, and 25 have also been slightly amended to make clear that the permanent public database is separated from the personal device. In addition, claim 27 is newly submitted directed to a device written using means plus function terminology corresponding to the actions recited in amended claim 1. No new matter is added.

Claim Rejections - 35 USC §103

Applicant notes at page 2 of the Action that the arguments presented in applicant's response of September 27, 2007 were found to be persuasive and that as a result, a new ground of rejection has been made by the Office in which the previously cited references (Mauro - US patent application 2002/0147920 and Craft - US patent application publication 2002/0150243) are further combined with US patent 6,978,022, Okimoto, et al (hereinafter Okimoto), for rejection of claims 1, 3, 4, 6, 8, 9, 11, 12, 14, 17-23, and 25 under 35 USC §103(a).

With regard to claim 1, the Office argues a combination of Mauro and Craft similar to the argument set forth in the Official Action of June 22, 2007 and cites Okimoto for disclosing that the secure processing point is separated from the personal device. Applicant respectfully disagrees.

The Present Invention

As set forth in the present application, there is a need for personal devices to include one or more device specific cryptographic keys where the number and types of these keys are dependent on the different applications included in the device, which

applications will differ between different users and their respective usage of the device. Furthermore, it is noted that it is difficult to perceive these numbers and types of keys that should be included in the device and therefore it is necessary to be able to store a variety of keys in a storage area of the device when initializing the device. Typically, most of these keys will be stored in some non-robust memory; that is, any memory in which information can be written and with the potential risk of losing any such information due to failure of the mechanism used for maintaining the information and the memory. As a consequence, in the case of a failure of the device that results in loss of the original stored keys, it is desired to be able to restore these keys in a device and, in particular, when transferring any secret keys or private keys for re-storage in the device, it is typically required to maintain secrecy and integrity of the transferred keys (specification, page 2, line 17 through page 3, line 2).

Thus, an object of the invention is to provide a method and system for managing, with reduced overhead, cryptographic keys that are specific to a personal device. It is noted that in an embodiment of the invention, a data package, including one or more cryptographic keys is transferred to a personal device from a secure processing point of a device assembly line in order to store device-specific cryptographic keys in the personal device. In response to the transfer data package, a back-up data package is received by the secure processing point from the personal device, which backup data package is the data package sent to the device, but encrypted with a unique secret key stored in a tamper-resistant secret storage of a chip included in the personal device. The secure processing point retrieves a unique chip identifier from the chip in the device and associates the unique chip identifier with the backup data package, after which the backup data package together with the associated unique chip identifier is stored in a permanent, global, public database (specification, page 4, lines 10-25).

By so doing, neither the device manufacturer nor any device administrator needs to maintain a secret database storing keys for decrypting backup data packages since the

backup data package can be decrypted by the device using the non-distributed unique secret chip key stored in the device if, for some reason, the data package sent to the device from the secure processing point is later lost or rendered inoperative (specification, page 5, lines 14 through page 6, line 3).

It is to this overall methodology that claim 1 is directed.

The Art Rejection

The Office asserts that Mauro teaches the action of retrieving in a secure processing point separated from and arranged in communication with the personal device, a unique chip identifier from a read-only storage of an integrated circuit chip included in the personal device (citing paragraph [0038] of Mauro).

Initially, it should be noted that Mauro is directed to techniques for providing secure processing and data storage for a wireless communication device, wherein a remote terminal includes a data processing unit, a main processor, and a secure unit. The data processing unit processes data for communication over a wireless link. The main processor provides control for the remote terminal and the secure unit includes a secure processor that performs the secure processing for the remote terminal and a memory that provides secure storage of data. The secure processor may include embedded read-only memory (ROM) that stores program instructions and parameters used for secure processing (Mauro, Abstract).

The referenced paragraph [0038] in Mauro describes Figure 3, where Figure 3 is a diagram of a specific embodiment of secure unit 240 of remote terminal 110 (see Figure 1). Therefore, ROM 252 is implemented within secure processor 250 where the secure processor 250 is operated without dependency on other external elements (Mauro paragraph [0038]). This is at variance to the requirement of the action recited in claim1 of retrieving in a secure processing point separated from and arranged in communication

with the personal device. Consequently, ROM 252 of secure processor 250 is part of the personal device, contrary to what is specifically recited in claim 1.

The Office further recites that the second action in claim 1; namely, the secure processing point storing a data package in the personal device, the data package including at least one cryptographic key, is taught by Mauro at paragraph [0034], lines 1-7; namely, a secure unit 240 to perform all secure processing and store all "sensitive" data by various cryptographic technique. Paragraph [0034] of Mauro discusses secure processing and data storage within secure unit 240 of remote terminal 110 and thus it is not equivalent to the secure processing point as set forth in claim 1 which stores a data package in the personal device, where the secure processing point is separated from and arranged in communication with the personal device. Thus, this aspect of claim 1 is not taught by Mauro.

Furthermore, it should be emphasized that Mauro has nothing to do with managing cryptographic keys that are specific to a personal device, but rather is directed to techniques for providing secure processing and data storage for a wireless communication device. Mauro has nothing to do with storing a backup data package which the personal device has received from the separated secure processing point, wherein the backup data package and an associated unique chip identifier is encrypted with a unique secret key stored in a tamper-resistant secret storage of an integrated circuit chip included in the personal device and further wherein the backup data package and associated unique chip identifier is maintained in a permanent public database separated from the personal device.

This latter aspect of claim 1 has been added in order to emphasize that the permanent public database is in fact separated from the personal device. This is clearly shown in Figure 1 of the present application and discussed in the specification, including the above-recited portions of the specification.

The Office further relies upon Craft for showing the next action of claim 1; namely, receiving at the secure processing point, and response to storing the data package, a backup data package from the personal device, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant storage of the chip, citing Craft, including paragraphs [0019] and [0021].

Initially, it should be noted that Craft is directed to a secure communication methodology, wherein a client device is configured to download application code and/or content data from a server operated by a service provider. Embedded within the client is a client private key, a client serial number, and a copy of a server public key. The client forms a request, which includes the client serial number, encrypts the request with the server public key, and sends the download request to the server. The server decrypts the request with the server's private key and authenticates the client. The received client serial number is used to search for a client public key that corresponds to the embedded client private key, whereby the server encrypts its response, which includes the requested information, with the client public key of the requesting client so that only the private key of the requesting client can decrypt the information downloaded from the server (Craft, Abstract).

Thus, the whole methodology of Craft is to allow a client device to request and receive information from a server in a reliable fashion. Paragraphs [0019] and [0021] of Craft in reference to Figures 2 and 4 discuss a flow chart by which a server receives an encrypted (with the server public key) client request message, decrypts the encrypted client request message with the server private key, retrieves the client serial number from the decrypted client request message, searches for the client public key associatively stored with the client serial number, retrieves the client public key, retrieves encrypted client authentication data from the decrypted client request message, decrypts encrypted client authentication data and verifies decrypted client authentication data all being performed by the server.

It is not seen how these actions of the server correspond to receiving a backup data package from the personal device, which backup data package is the data package encrypted with a unique secret key stored in a tamper-resistant secret storage of the chip. Rather, it shows that server can receive an encrypted message from the client, wherein the encrypted message contains the necessary client serial number and such that it is encrypted with the server's public key thereby allowing the server to decrypt the message with the server's private key so as to authenticate the client. There is no teaching or suggestion of receiving a backup data package corresponding to the data package sent to the personal device from the secure processing point (server).

The Office further relies on paragraphs [0041] and [0043] of Craft for asserting that Craft teaches associating the unique chip identifier with the received backup data package and storing the backup data package and the associated unique chip identifier in a permanent public database. What paragraphs [0041] and [0043] of Craft are directed to is that the client CPU chip is a special-purpose client-system processor chip which has a cryptographic unit that has been manufactured to contain programmable memory storage. Prior to releasing the CPU chip, the manufacturer permanently embeds a client serial number, the assigned client private key, and the server public key in the CPU chip.

As shown in Figure 2, the client CPU chip contains a cryptographic unit which includes the client serial number 216, the client private key 218, and the server public key 220. Even if as argued by the Office, the client serial number 216 in Craft is equivalent to a unique chip identifier and a server's client public key data store 222 is equivalent to a permanent public database, there is still no showing in Craft of the server 208 receiving a backup data package from the personal device, wherein the backup data package is the data package received by the personal device from the secure processing point, but encrypted with a unique secret chip key stored in a tamper-resistant secret storage of the integrated circuit chip included in the personal device.

Rather, Craft merely discloses that the client serial number is used to form a request to the server, the request encrypted with the server's public key for purposes of server authentication of the client. There is absolutely no disclosure in Craft of receiving a backup data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage of an integrated circuit chip included in the personal device. Furthermore, the fact that paragraph [0043] of Craft discloses that the manufacturer of the client CPU chip may then destroy any existing copies of the client private key 218 while the client serial number 216 and the client public key corresponding to the client private key 218 are associatively retained for subsequent use and deployment such as by storing them within the server's client public key data store 22, at best is for purposes of retrieving the client serial number and the client public key corresponding to a client private key, but is not for purposes of allowing the personal device to retrieve a data package which was previously sent to it by a secure processing point in case the data previously received becomes damaged or destroyed for some reason.

It is therefore not seen how paragraphs [0041] and [0043] of Craft disclose these particular actions recited in claim 1.

Finally, the Office relies upon Okimoto and, in particular, column 3, line 67 through column 4, line 1, as well as column 5, lines 52-53, for disclosing that a secure processing point is separated from a personal device.

Okimoto is an encryption renewal system and for registration and remote activation of an encryption device specifically associated with a system for securely delivering encrypted content on demand with access control, such as associated with cable systems and the like. It is disclosed in Okimoto that content is encrypted once at a centralized facility and is usable at different point-to-point systems through use of an encryption renewal system (ERS) for performing entitlement control messages (ECM) retrofitting to keep pre-encrypted contents usable (Okimoto, page 3, lines 26-28).

With respect to the encryption renewal service, it is disclosed that the renewal service is separated into two or more computing platforms to protect the data and that the second platform is physically separated to handle secure processing. The fact that an encryption renewal system uses two or more computing platforms in no way is suggestive of a secure processing point separated from and arranged in communication with a personal device so as to store a data package in the personal device, as well as to receive a backup data package from the personal device encrypted using a secret chip key stored in a tamper-resistant secret storage of an integrated circuit chip included in the personal device.

Overall, the combination as asserted by the Office appears to be nothing more than hindsight reconstruction in order to try to arrive at the actions recited in claim 1.

Furthermore, claim 1 has been slightly amended to make clear that the chip referred to in the receiving action is the integrated circuit chip previously recited which is included in the personal device and further that the permanent public database is separated from the personal device.

For all of the foregoing reasons, it is respectfully submitted that claim 1 is not suggested by a combination of Mauro and Craft further in view of Okimoto.

For similar reasons as those presented above with respect to amended claim 1, it is respectfully submitted that independent system claim 9, independent method claim 17, independent personal device claim 18, and independent secure processing point claim 25 are also not anticipated by Mauro in view of Craft in view of Okimoto since each of these claims recite features corresponding to those recited above with respect to claim 1.

Furthermore, dependent claims 3, 4, 6, 8, 11, 12, 14, and 19-23 are also further distinguished over Mauro in view of Craft further in view of Okimoto at least in view of their dependency from independent claims which are distinguished over the cited art.

At page 14, claims 2, 5, 8, 10, 13, 16, 24, and 26 are rejected under 35 USC §103(a) as unpatentable over Mauro in view of Craft further in view of Okimoto further in

view of US patent application publication 2002/0157002, Messerges, et al. Each of these claims is dependent upon an independent claim which is believed to be distinguished over the cited art and therefore each of these claims is believed to be further distinguished over the cited art at least in view of such dependency.

Furthermore, newly submitted independent claim 27 corresponds to method claim 1, but written as a device using means plus function terminology. For the reasons presented above with respect to claim 1, claim 27 is also believed to be allowable.

In view of the foregoing, it is respectfully submitted that the present application as amended is in condition for allowance and such action is earnestly solicited.

Respectfully submitted,

Dated: June 5, 2008

Alfred A. Fressola
Attorney for Applicant
Registration No. 27,550

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955